OUTLINE
2026

WITH TAWANA
. BUILD SKILLS.
CHANGE YOUR FUTURE

TAWANA
TECHNOLOGY

WWW.TAWANATECHNOLOGY.COM

+93788077685

Security+

OUTLINE

TAWANA TECHNOLOGY

2026

www.tawanatechnology.com

Security+

1 Module: General Security Concepts 12%

- CIA triad
- Security Controls (Technical, Managerial, Operational, Physical)
- Risk concepts (Threat, Vulnerability, Risk, impact)
- Zero Trust model
- Basic Cryptographic concepts
- Physical Security concepts

2 Module: Threats, Vulnerability, and Mitigations 22%

- Malware types (Virus, Ransomware, Trojan, etc.)
- Social Engineering Attacks
- Network Attacks (Dos/DDos, MITM, Replay, DNS attack)
- Web Application Attack
- Advance Persistent Threats (APT)
- Vulnerability Scanning and Penetration Testing
- Mitigation Techniques

3 Module: Security Architecture 18%

- Secure Network Architecture
- Network Segmentation and VLANs
- Firewalls, IDS/IPS
- Cloud Security Concepts
- Endpoint Security
- Secure System Design
- PKI and Digital certificates

4 Module: Security Operation 28%

- Monitoring and Logging
- SIEM
- Incident Response Procedures
- Digital Forensics Basics
- Disaster Recovery (DR) and Business Continuity (BC)
- Patch Management
- Backup Concepts

5 Module: Security Program Management and Oversight 20%

- Governance
- Security Policies and Procedures
- Compliance Frameworks (GDPR, HIPAA, PCI-DCC)
- Risk Management Frameworks
- Security Awareness Training
- Third-party/Vendor Risk Management
- Legal and Ethical Considerations

Week 1st:

Session1: introduction to Security+, What Happened in World, What is Security,CIA triad,

Confidentiality, Integrity, availability, Security Controls, Technical Controls (logical controls), Managerial Controls (administrative Controls), Operational Controls, Physical Controls

Session2: Threats, Attack, Vulnerability, Risk, Zero Trust model, Why Zero Trust, Zero trust Principle, Core Component of Zero Trust. AAA

Session3: Cryptography, Physical Security Concepts, What are Physical Security?, Core Physical Security, Common Physical Security Controls

Session4: Malware, type of Malware, Type of Malware, Virus, Worms, Trojans, Ransomware, Spyware, Adware, Rootkit, keyloggers, Backdoor, Botnet, Potentially (unwanted programs), Fileless virus, Command and control, Crypto Malware, Logic bombs, Remote access trojan(RAT)

Session5: Type of cybersecurity attack, Social Engineering Attack, Phishing Attack, Smishing, Vishing, Spam and SPIM,   Spear Phasing, Dumpster diving attack, Shoulder surfing, Tailgating, Pharming attack, Eliciting information, Whaling attack

Week 2nd:

Session1: Reconnaissance, Doing some practical Reconnaissance,   Hoax email attack, Impersonation, Watering hole attack, Typo Squatting, Pretexting, Influence campaigns, Principles(reasons for effectiveness), Familiarity, Trust, Urgency, Authority, Intimidation, Consensus, Scarcity

Session2: Network Attacks, Common Types of Network Attacks, Denial-of-Service (DoS), DDoS (Distributed Denial of Service), Type of DDoS attack, On-path Attack (MITM attack), Packet Sniffing, Spoofing

Session3: Session Hijacking, (DNS) spoofing attack, Replay attack, Eavesdropping, Wireless, Bluejacking, Disassociation attack, Jamming attacks, RFID

Session4: NFC, Initialization vector, Layer2 attack, (ARP)poisoning attack, Mac Cloning attack, Domain Hijacking, Uniform Resource Locator (URL) redirection , Application, Operational Technology(OT),

Session5: practical and recap all lessons

Week 3rd:

Session1: Password attack, Dictionary Attack, Spraying, Brute Force, Offline Password Attack, Online attack, Rainbow Table, Physical attacks, Malicious Universal, Malicious Flash Drive, Card Cloning attack, Skimmers attack, Supply-chain attacks, Cryptographic attacks, Collision, Downgrade

Session2:   Web application Attacks, Privilege escalation, (SQL), Injections, Cross-Site(xss), Cross-site scripting(xss), Type of XSS, Request Forgeries, Command Injection, File Inclusion (LFI / RFI)

Session3: Directory traversal attack, Directory Traversal, Broken Authentication, Security Misconfiguration, Insecure Direct Object reference (IDOR), XML, Buffer overflows, Race conditions, Error handling, input handling, Server-side, Application programming interface, Memory leak, Secure Sockets layer(SSL) stripping attack, Driver Manipulation attack, Skimming, Pass The Hash attack

Session4: Prevention Methods for Web Attacks, Malicious code or script execution, PowerShell, Python, Bash, Macros, VBA

Session5: recap all from 1st week up to 3rd week,

Week 4th:

Session1: Projects from Student own research

Session2: Actors and Threats, (APT), Who are Common Targets, Typical APT Attack Stages, APT vs Normal Attack, How to Defend Against APT

Session3: Insider threat, State actors, Hacktivists, Criminal syndicates, Hackers, Type of hacker, Script kiddies, Type of Hacker(hat), White hat hacker, Black hat hacker, Gray hat hacker, Shadow IT,

Session4: Vulnerability Scanning, Command Vulnerability Exposures(CVE), Common vulnerability(CVSS), Common Tools (Concept level), Attributes of actors, Internal/External actor, Level of sophistication/capability, intent/motivation, Resources/funding, Vectors

Session5: exam

Week 5th:

Session1: Threat Vector, Direct access, Web Application, Scan Network , False positive and Negative, Vulnerability scans, Vulnerability Scan step, Vulnerability databases, Practical Vulnerability Scan

Session2: Cloud-based vs. on-premises vulnerabilities, Zero-day, Weak configurations, Open permission, Unsecure Root account, Weak encryption, Unsecure protocols, Default setting, Open port and service, Supply chain vulnerability, Application risk, Outsourced code development, weak patch management, Session3: Firmware, Operating system(OS), Legacy platform, Impacts of vulnerability, Result of vulnerability in system, Data loss, Data breaches, Data exfiltration, Identity theft, Financial loss, Damage to reputation, Availability loss

Session4: Penetration testing, Penetration Testing (Pentesting), Characteristics, What Pentesters Do, Black-box, Gray-box, white-box penetrating test, Rules of engagement, Privilege escalation, Persistence, Covering track, Bug bounty, Pivoting, Passive and active reconnaissance, Active reconnaissance, Drones, Foot printing

Session5: working on students practical skill

Week 6th:

Session1: Type of penetration testing team, Key Difference, Mitigation Techniques, Threat intelligence sources, OSINT, Closed/Proprietary, Public/private information- sharing centers, File/Code Repositories, Research sources, Vendor websites , Vulnerability feeds, Threat feeds

Session2: Security Architecture, What is Security Architecture, CIA Triad – Core of Security, Defense in Depth, More Tips, Three-Tier Architecture, DMZ Design, Load Balancing, Network Segmentation Definition, Logical Segmentation, Physical Segmentation

Session3: VLAN Explanation, Microsegmentation, Firewall Overview, IDS Definition, IPS Definition, Cloud Security Concepts, Cloud Computing Definition, IaaS Model, PaaS Model, SaaS Model

Session4: Cloud Deployment Models, Cloud threat, Cloud Risks, Cloud Security Controls, Signature vs Anomaly Detection, Endpoint Definition, What does Endpoint Security Do?, Antivirus and Anti-malware, System Hardening, Secure Coding,

Session5: PKI Overview, Asymmetric Cryptography, Certificate Authority (CA), Registration Authority (RA), CRL and OCSP, Digital Certificate Contents

Week 7th:

Session1: Projects from Student own research

Session2: Security Operations Overview, What is SOC (Security Operations Center), Monitoring Definition, Why Monitoring Is Important, Type of Monitoring, Monitoring Tools, Logging Definition, Why Logging Is Important, Log review, Configure review, Type of Logs

Session3: SIEM Overview, Security information event management, Review reports, Packet capture, Data inputs, User behavior analysis, Sentiment analysis, Security monitoring, Log aggregation, Why SIEM Is Important, What SIEM Collects, Core Function of SIEM, What Is correlation

Session4: Incident Response Procedure, Why Incident Response Is Important, The 6 Phases of Incident Response (Preparation), Digital Forensics, Core Principles of Digital Forensics

Session5: Digital Forensics Process, Types of Digital Evidence, Business Continuity, Disaster Recovery, Patch Management, Patch Management Lifecycle, Backup Concepts, Backup Security

Week 8th:

Session1: Governance, Why Governance Is Important, Key Governance Components, Roles in Governance, Security Policies and Procedures, Common Security Policies, Procedures

Session2: Compliance Frameworks, Why Compliance Is Important, Major Compliance Frameworks,

GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), PCI DSS (Payment Card Industry Data Security Standard),

Session3: Risk Management Frameworks, Risk Management Steps, Common Risk Framework, Security Awareness Training, Why It Is Important, Training Topics, Training Methods

Session4: Third-Party / Vendor Risk Management, Third-port Risk, Vendor management risk, Lack of vendor support, Why Third-Party Risk Is Dangerous, Vendor Risk Management Process

Session5: Legal and Ethical Considerations, Ethics vs Law

Our Partners

Tawana

Best Tecnology center

2026

Tawana: The Key to the World of Technology

STUDENT FEEDBACK

Our students' opinions about Tawana Technology

MOHAMMAD SHARIF BAKHTYARY

"Tawana Technology is a trusted institute with a strong background in technology, offering advanced curricula and modern methods—especially in cyber—to help learners enhance their skills."

Datacenter Specialist at UST Global

TAWAB FAYAZI FORMER

"Tawana Technology is a leading institute for learning technology. Its students excel in job markets and competitions locally and internationally. I highly recommend it to anyone eager to grow their skills."

I.T DIRECTOR OF AFGHANISTAN INDEPENDENT HUMAN RIGHTS COMMISSION

SUHRAB TOTAKHAIL

"Tawana Technology is a leading Center for learning technology. Its students excel in job markets and competitions locally and internationally. I highly recommend it to anyone eager to grow their skills."

IT ANALYST ETISALAT AFGHANISTAN

2026

TAWANA OUTILINE

Presented By :

Tawana team